Coding and Cryptography Spring 2014

Tutorial Project #1

Due at the end of class.

On Friday, we learned how to decode a linear code using 'syndromes'. Make sure someone in your working group attended class on Friday, and get out their notes, where there is an example. Your text also has the same example on page 412.

Exercise 1. Here is the generating matrix G for a binary code (i.e. the code is generated by the rows of this matrix).

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}.$$

Determine the parameters of this linear binary code. What is its length n? What is its dimension k? How many (M) codewords does it have? What is its minimum distance d (hint: Hamming weight)? Finally, how many errors can it detect and correct?

length $n = 14$

dimension $k = 10$

codewords $M = 2^{10}$

min. dist $d = 3$

detects 2 errors

corrects 1 error

Exercise 2. Write out H, the parity check matrix for this code.

$$\begin{pmatrix} 1&1&1&0&0&0&0&1&1&1&1&0&0&0&0 \\ 1&1&0&1&0&1&1&0&0&1&0&1&0&0&0 \\ 1&0&1&1&1&0&1&0&1&0&0&0&1&0&0 \\ 0&1&1&1&1&1&0&1&0&0&0&0&0&1&0 \end{pmatrix}$$

Exercise 3. For the code above, give six examples of codewords (don't just pick rows of the matrix, pick some non-trivial linear combinations of rows!).

eg. 1 1 0 0 0 0 0 0 0 0 0 0 0 1 1 ← by adding 1st 2 rows

0 0 0 0 0 0 0 0 0 1 1 0 1 1 0 ← by adding last 2

Exercise 4. For five of the six examples above, randomly change one digit. Leave one of them alone. (This simulates transmission over a noisy channel.) Check with your teacher that you've done this correctly (right now!). After your teacher has checked it's correct, give the resulting "transmitted messages" to another group, and get their "transmitted messages".

V_1 = 1 1 0 1 0 0 0 0 0 0 0 1 1 changed

V_2 = 0 0 0 0 0 0 0 0 1 1 0 1 1 0 not

Exercise 5. For the transmitted messages you received, compute the syndrome of each one using H^T. (Hint: this should be a vector with four entries.) Using the result, identify the transmitted message which got through without any errors occurring.

$$H^T = \begin{pmatrix} 1&1&1&0 \\ 1&1&0&1 \\ 1&0&1&1 \\ 0&1&1&1 \\ 0&0&1&1 \\ 0&1&0&1 \\ 0&1&1&0 \\ 1&0&0&1 \\ 1&0&1&0 \\ 1&1&0&0 \\ 1&0&0&0 \\ 0&1&0&0 \\ 0&0&1&0 \\ 0&0&0&1 \end{pmatrix}$$

$V_1 H^T = (0\ 1\ 1\ 1)$ -

$V_2 H^T = (0\ 0\ 0\ 0) \Rightarrow$ Codeword, no errors

Exercise 6. For each of the other vectors v (the ones that have errors), do the following:

1. Find the shortest codeword that has the same syndrome as v. That is, by looking at the matrices you have in hand, divine a ~~codeword~~ vector that has the lowest Hamming weight and results in that same syndrome. (Hint: this involves thinking, not calculating; this is the 'coset leader'. In particular, you shouldn't have to write out a whole table to do this. The table would be tooooooo biiiiiiiiiig.).

2. Assume that the received message was created by one error. What was the message that was sent? (Hint: add a codeword + the short vector of the previous part)

Fill out a table:

4th spot has a '1'

received message	syndrome	coset leader	codeword sent	position error occurred	which column(s) of H equals the syndrome?
v_1	0110	0000000000 00000	1101000000 00011	4	4th
v_2	0000	0000000000 0000000 ↑ all 0's	v_2	—	—

Make a conjecture about an easy way to decode based on the table above (particularly the last column). Explain why it works. Finally, check with the other group that you correctly error-corrected the other group's messages.

Conj. look for syndrome as a row of H^T; this is position of error.

Expl. The vector of 0's w/ a single 1 in that position has same syndrome. It has Hamming wt 1. It is the coset leader.

Exercise 7. If time remains in class, try to construct your own efficient linear codes. If you want to be able to send 2 information bits, how many parity check digits do you need to make a code that can correct one error? To send 3 information bits, how many? To send 4? (Write out the matrices.) Can you do better if you work over a larger finite field like $\mathbf{Z}/3\mathbf{Z}$? Can you construct a binary linear $[9, 5, 3]$ code? Can you construct a $[8, 2, 5]$ (this will correct two errors!?!)?

Have fun.